

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200309085-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): David Andrew Thomas

Confirmation No.: 1203

Application No.: 10/678,936

Examiner: Minh Dinh

Filing Date: October 3, 2003

Group Art Unit: 2132

Title: METHOD AND SYSTEM FOR FILE DOWNLOADS TO PORTABLE COMPUTING DEVICES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on January 18, 2008.

☒ The fee for filing this Appeal Brief is \$510.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☒ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☒ 1st Month
\$120

☐ 2nd Month
\$460

☐ 3rd Month
\$1050

☐ 4th Month
\$1640

☐ The extension fee has already been filed in this application.

☐ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 510. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

Date: April 18, 2008

I hereby certify that this document is being filed by personal delivery to the Customer Service Window Randolph Building, 401 Dulany Street Alexandria, VA 22314, of the United States Patent & Trademark Office on the date indicated above.

By: Patrick C. Keane Reg. No. 32,858
(Attorney Signature and Reg. No.)

Respectfully submitted,

David Andrew Thomas

By: Patrick C. Keane

Patrick C. Keane

Attorney/Agent for Applicant(s)

Reg No. : 32,858

Date : April 18, 2008

Telephone : (703) 838-6522

Table of Contents

I.	Real Party in Interest.....	2
II.	Related Appeals and Interferences	2
III.	Status of Claims	2
IV.	Status of Amendments.....	2
V.	Summary Claimed Subject Matter.....	2
VI.	Grounds of Rejection to be Reviewed on Appeal.....	6
VII.	Argument	7
VIII.	Claims Appendix	11
IX.	Evidence Appendix	11
X.	Related Proceedings Appendix.....	11

I. Real Party in Interest

The present application is assigned to Hewlett-Packard Development Company, L.P. Hewlett-Packard Development Company, L.P. is the real party in interest, and is the assignee of the present Application No. 10/668,736.

II. Related Appeals and Interferences

The Appellants' legal representative or assignee, does not know of any other appeal or interference which will affect or be directly affected by or have bearing on the Board's decision in this pending appeal.

III. Status of Claims

Claims 1-58 remain pending. Claims 11-27 and 38-54 have been withdrawn following a restriction requirement. Thus, independent claims 1 and 28, along with dependent claims 2-10, 29-37 and 55-58 have been finally rejected and are the subject of this appeal.

IV. Status of Amendments

All prior amendments, including the last amendment filed June 28, 2007, have been entered. There are no pending amendments.

V. Summary Claimed Subject Matter

The subject matter of each independent claim on appeal (claims 1 and 28), as well as means-plus-function dependent claims 30-33, is cross-referenced to the specification and/or drawing figures in the following table:

1. (Previously Presented) A method for transferring files, comprising:	E.g., Figs. 2-10
receiving a request to transfer a file;	E.g., Fig. 3, Step 304; Spec. pg. 7, lines 12-13; Fig. 5, Step 512; pg. 8, lines 30-31; pg. 9, lines 9-18; pg. 10, lines 8-9

locating the requested file stored in a memory;	E.g., pg. 10, lines 9-10
computing a unique identifier corresponding to the requested file;	E.g., pg. 10, line 2 (MD5 checksum) and lines 18-21
choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file;	E.g., Fig. 6, Step 610; pg. 10, lines 18-21
encrypting the first key, K_1 , and the unique identifier with a second key, K_2 , to generate a first value;	E.g., Fig. 6, Step 610; pg. 10, lines 21-23; pg. 12, lines 1-3
encrypting the requested file with the first key, K_1 , to generate a second value; and	E.g., Fig. 6, Step 610; pg. 10, lines 18-21; pg. 12, lines 1-3
transferring the first and second values.	E.g., Fig. 6, Step 612; pg. 10, lines 24-25; Fig. 7, Step, 706; page 11, lines 3-13
28. (Previously Presented) An apparatus for transferring binary files, comprising:	E.g., Fig. 2, System 200, spec. pg. 6, lines 9-10
means for receiving a request to transfer a file;	E.g., Fig. 2, Server 204, spec. pg. 6, lines 19-21; Fig. 5, step 512, pg. 8, lines 30-31; pg. 9, lines 9-18; Fig. 6, step 602, spec. pg 10, lines 8-9
means for locating the requested file stored in a memory;	E.g., Fig. 2, Server 204, spec. pg. 10, lines 9-10
means for computing a unique identifier corresponding to the requested file;	E.g., Fig. 2, Server 204, spec. pg. 10, lines 18-21
means for choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file;	E.g., Fig. 2, Server 204, spec. pg. 10, line 2 and lines 18-21
means for encrypting the first key, K_1 , and the unique identifier with a second key, K_2 , to generate a first value;	E.g., Fig. 2, Server 204, spec. pg. 10, lines 21-23; server 206 or 208; spec. pg. 12, lines 1-3
means for encrypting the requested file with the first key, K_1 , to generate a second value; and	E.g., Fig. 2, Server 204, spec. pg. 10, lines 18-21; server 206 or 208; spec. pg. 12, lines 1-3
means for transferring the first and second values.	E.g., Fig. 2, Server 204, spec. pg. 10, lines 18-21; server 206 or 208; spec. pg. 12, lines 1-3
30. (ORIGINAL) The apparatus of claim 28, further comprising means for transferring the first key, K_1 , upon a payment being made.	E.g., Fig. 2, server 208, pg. 13, lines 13-15
31. (ORIGINAL) The apparatus of claim 30, further means for comprising decrypting the second value with the first	E.g., Fig. 2, PDA 202

key, K ₁ , to generate the requested file.	
32. (ORIGINAL) The apparatus of claim 28, further comprising means for interrupting the transmission of the second value.	E.g., Fig. 6, Step 620; spec. pg. 10, last para. to pg. 11, line 2; Fig. 2, server 204
33. (ORIGINAL) The apparatus of claim 32, further comprising means for continuing the transmission of the second value without retransferring the entire second value.	E.g., Fig. 2m PDA 202, server 204 at different location than other server initially used for transmitting; pg. 7, method 700; spec. pg. 11, lines 3-6

The presently claimed invention is directed to methods and systems for transferring files (e.g., downloading digital, such as files containing audio and video information. Specification page 2, lines 21-24 state:

Several schemes are described for handling a large file such as that of the video component of a digital movie. Where the video component is downloaded separately from an audio component, it can be downloaded over several sessions.

Large digital media files, such as the Figure 1 block 100 described in the last paragraph on specification page 4 (e.g., page 4, lines 28-30), can be downloaded in a progressive manner by allowing for a transfer of such digital media to occur over several sessions which can occur at multiple locations (e.g., multiple locations of temporary Internet access; so called "hot spots"). See specification page 5, lines 2-3.

In downloading the Figure 1 block 100 (representing a large audio/video digital data file), exemplary embodiments can download components (e.g., Figure 1 blocks 102, 104, 106, 108) progressively. The Figure 1, block 100 can include a video portion that is downloaded separately from an audio component.

Figure 2 shows a system 200, as described on specification page 6, lines 9 et seq, wherein a mobile PDA 202 can wirelessly communicate with multiple file servers 204 as the PDA moves from one access point ("hot spot") to another (see

spec. pg. 11, lines 4-7). The file server 204 can make multimedia files available to PDA 202 via file downloads. A payment server 208 described on specification page 7, lines 3-5 can accept payment and release an appropriate decryption key that provides access to a downloaded file.

Figure 5 shows an exemplary method 500 for PDA 202 to access file server 204 via a wireless access point. Once accessed, a media file can be downloaded in, for example, a manner as described with respect to Fig. 6, on specification page 9, fourth paragraph.

To enable such a multisession transfer, exemplary embodiments exploit the use of a "unique identifier" corresponding to a requested file. As described with respect to Fig. 6, on specification page 10, the unique identifier can include use of, for example, an MD5 checksum (page 10, line 2). A "first key K", which is unique to the particular transfer of the requested file (i.e., a transfer which can occur over multiple varied sessions) is described at page 10, lines 18-21. A "second key K₂" is used to encrypt the first key K₁ and the unique identifier. See Fig. 6, step 610 and specification page 10, third paragraph (page 10, lines 18-23).

In an exemplary embodiment, upon receiving a request to transfer a file, a file server locates the requested file in its memory. For verification purposes, a unique identifier is computed for the requested file, such as the MD5 checksum, of the digital file. Thereafter, an encryption key, K₁, is chosen. Using a second key, K₂, the first key and the unique identifier are encrypted, and the requested file is encrypted using the first key. Both these encrypted values are then transmitted (see block 612).

Where the file transfer is interrupted, the Fig. 7 process 700 is initiated in step 620. The Figure 7 method is described at specification page 11, lines 3-6. Authenticity of a transferred file can be verified via the Figure 8 method (see specification page 12, second full paragraph).

For a transferred file to be useful, the Figure 2 PDA 202 receives a decryption key K from the payment server 208 (see specification page 12, last paragraph, lines 6-9). Subsequently, (for example, after payment is received) in Figure 8, block 816, an unencrypted form of the first key is transmitted as described at specification page

13, lines 13-15. The first key can be used to decrypt the requested file to unlock full functionality of the requested file at the PDA 202.

The foregoing features are broadly encompassed by independent claim 1, which recites a method for transferring files, comprising, among other features, receiving a request to transfer a file; locating the requested file stored in a memory; computing a unique identifier corresponding to the requested file; choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file; encrypting the first key, K_1 , and the unique identifier with a second key, K_2 , to generate a first value; encrypting the requested file with the first key, K_1 , to generate a second value; and transferring the first and second values. Independent claim 28 recites similar features.

As broadly encompassed by claim 1, the first key, K_1 , is unique to the particular transfer of the requested file, and is encrypted by the second key K_2 . K_1 is used to achieve a complete file transfer despite the occurrence of interruptions (see page 11, lines 10-15). However, the same file requested from the same or different hot spot at a different time will have a different first key. In this manner, progressive transfer of the file can be achieved as a mobile PDA moves from one "hot spot" to another.

VI. Grounds of Rejection to be Reviewed on Appeal

- A. Whether The Examiner Has Established A Prima Facie Case Of Obviousness In Rejecting Claims 1-4, 7, 28-31 and 34 Under 35 U.S.C. § 103(a) As Being Unpatentable Over U.S. Patent Publication No. 2002/0107806 (Higachi et al) In View Of U.S. Patent No. 7,242,766 (Lyle)?
- B. Whether The Examiner Has Established A Prima Facie Case Of Obviousness In Rejecting Claims 5-6 and 32-33 Under 35 U.S.C. § 103(a) As Being Unpatentable Over Higachi et al and Lyle In Further View of U.S. Patent No. 6,963,923 (Bennett)?
- C. Whether The Examiner Has Established A Prima Facie Case Of Obviousness In Rejecting Claims 8-10 and 35-37 Under 35 U.S.C. § 103(a) As Being Unpatentable Over Higachi et al and Lyle In Further View of U.S. Patent No. 6,807,623 (Carpentier et al)?

- D. Whether The Examiner Has Established A Prima Facie Case Of Obviousness In Rejecting Claims 55-58 Under 35 U.S.C. § 103(a) As Being Unpatentable Over Higachi et al and Lyle In Further View of U.S. Patent Publication No. 2002/0076043 (Van Der Vleuten)?

VII. Argument

- A. Claims 1-4, 7, 28-31 and 34 Under 35 U.S.C. § 103(a) Are Patentably Distinct Over U.S. Patent Publication No. 2002/0107806 (Higachi et al) In View Of U.S. Patent No. 7,242,766 (Lyle) Because No Prima Facie Case Of Obviousness Has Been Established With Regard To Independent Claims 1 and 28

In numbered paragraph 6 on page 3 of the Final Office Action, independent claims 1 and 28, along with various dependent claims, are rejected as being unpatentable over the Higashi et al document (U.S. Publication No. 2002/0107806) in view of the Lyle patent (U.S. Patent No. 7,242,766). Applicants' independent claims 1 and 28 are patentable over the Higashi et al and Lyle documents because these documents neither teach or suggest, among other features, Appellant's claim 1 features of choosing a first key, K_1 wherein the first key is unique to the particular transfer of the requested file; and encrypting the first key K_1 , and the unique identifier with a second key K_2 .

On page 4 of the Office Action, the Examiner asserts:

Higashi does not disclose that the encryption key K_1 is unique to the particular transfer of the requested file. Lyle discloses a method for encrypting requested content wherein the encryption/decryption key (i.e., a session key) is unique to the particular transfer of the requested content (col. 22, lines 38-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Higashi method such that the encryption key K_1 is unique to the particular transfer of the requested file, as taught by Lyle. Such an encryption/decryption key would vary from one transaction to the next.

However, neither of the documents relied upon by the Examiner teach or suggest using Appellants' claimed key K_2 to encrypt a first key K_1 , having the features recited in claims 1 and 28.

The Higashi document discloses a system and method to manage a digital content such as music and videos distributed via communications or broadcasting in a manner to manage rights of the content and to control the usage of the content such as to restrict the number of times to reproduce the content. Figure 2, relied upon by the Examiner, illustrates choosing a content key used to encrypt the requested file. The Examiner alleges that the content key constitutes Appellants' first key, K_1 . The Higashi document discloses that the content key is related to the content itself. *See paragraph [0074]*. The content key does not change depending on the particular file request transfer. Thus, as acknowledged by the Examiner, the Higashi document does not teach or suggest Appellants' claimed feature of choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file, as recited in claims 1 and 28.

The Lyle patent does not overcome the deficiencies of Higashi, and therefore no prima facie case of obviousness has been established. Lyle discloses, as a first alternative, using a public key allocated to receiver 15 to encrypt content delivered by a content source 11 to the receiver 15. The receiver 15 can then use a private key stored in the receiver to decrypt the content. *See Col. 22, lines 30-35*. As a second alternative, the content is encrypted with a symmetric protocol and includes sufficient information to allow receiver 15 to generate, look up or otherwise obtain the necessary key for decrypting the content. *See Col. 22, lines 35-39*. As a third alternative, the content "is encrypted in a manner that requires a session key (that varies from one transaction to the next) in order to decrypt [the content]". *Col. 22, lines 39-42 (underlining added)*. It is this last alternative that the Examiner relies upon. However, this third alternative of Lyle merely suggests using a so-called "session key" to replace the public key of the first alternative when encrypting the content.

The third alternative of the Lyle patent relied upon by the Examiner, even when considered in combination with the disclosure of the Higashi patent would not have resulted in the presently claimed invention. In this third embodiment, a so-

called session key alone is used to encrypt content delivered to receiver 15. There would have been no teaching, suggesting or motivation to have used such a session key to encrypt the content of Lyle and to then use a second key to encrypt the session key. At best, the session key of Lyle would have been used to replace the content key and the public key of Higashi in the manner specifically described by Lyle in column 22. Even if the session key of Lyle is considered a first key (e.g., Appellant's claimed first key K_1) which is unique to a particular transfer of a requested file, neither Higashi nor Lyle teach or suggest encrypting such a session key (and Appellants' claimed unique identifier) with a second key (e.g., Appellants' claimed second key K_2).

Moreover, the "session key" of Lyle is a key that is unique to a given session with a given content source, and this key "varies from one transaction to the next" (Lyle, col. 22, line 41 (underlining added)). In contrast, Appellants' claimed "first key, K_1 " "is unique to a particular transfer (not just a single transaction) of a requested file" (claims 1, 28), and will remain valid over multiple transactions with different servers (e.g., as a mobile device establishes connection with different servers). See specification page 11, lines 10-15 and Figure 7. Such features allow for, among other features, the same file to be progressively downloaded as described, for example, with respect to Appellants' Figures 6 and 7 as described on specification pages 9-11.

Independent claim 1 is therefore allowable over the Higashi document. Independent claim 28 recites similar features and is also allowable. Claims 2-4, 7, 29-31 and 34 depend from these independent claims and recite further distinguishing features, and therefore, are allowable.

B. Claims 5-6 and 32-33 Under 35 U.S.C. § 103(a) Are Patentably Distinct Over Higashi et al and Lyle In Further View of U.S. Patent No. 6,963,923 (Bennett) Because No Prima Facie Case Of Obviousness Has Been Established With Regard To Independent Claims 1 and 28

In numbered paragraph 7 on page 4 of the Office Action, claims 5-6 and 32-33 are rejected as being unpatentable over the Higashi and Lyle documents, and in further view of Bennett (U.S. Patent 6,963,923). The Bennett document does not

overcome the above-noted deficiencies of the Higashi and Lyle documents. Because claims 5-6 and 32-33 recite additional features, these claims are allowable.

- C. Claims 8-10 and 35-37 Under 35 U.S.C. § 103(a) Are Patentably Distinct Over Higachi et al and Lyle In Further View of U.S. Patent No. 6,807,623 (Carpentier et al) Because No Prima Facie Case Of Obviousness Has Been Established With Regard To Independent Claims 1 and 28

In numbered paragraph 8 on page 5 of the Office Action, claims 8-10 and 35-37 are rejected as being unpatentable over the Higashi and Lyle document in view of Carpentier et al. (U.S. Patent 6,807,632). The Carpentier document does not overcome the above-noted deficiencies of the Higashi document. Accordingly, these claims which depend from claims 1 and 28 are allowable.

- D. Claims 55-58 Under 35 U.S.C. § 103(a) Are Patentably Distinct Over Higachi et al and Lyle In Further View of U.S. Patent Publication No. 2002/0076043 (Van Der Vleuten) Because No Prima Facie Case Of Obviousness Has Been Established With Regard To Independent Claims 1 and 28

The newly added Van Der Vleuten document does not overcome the deficiencies of the Higachi et al and Lyle documents discussed with respect to claims 1 and 28. Accordingly, claims 55-58 are allowable.

CONCLUSION

The Examiner has failed to establish a prima facie case of obviousness in finally rejecting independent claims 1 and 28, or the claims which depend therefrom. Reversal of the Examiner's rejection, and allowance of the present application, are therefore requested.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

See attached Evidence Appendix for copies of evidence relied upon by Appellant.

X. Related Proceedings Appendix

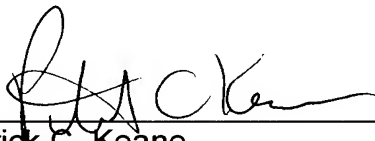
See attached Related Proceedings Appendix for copies of decisions identified in Section II, supra.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date April 18, 2008

By:



Patrick C. Keane
Registration No. 32858

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. (Previously Presented) A method for transferring files, comprising:
receiving a request to transfer a file;
locating the requested file stored in a memory;
computing a unique identifier corresponding to the requested file;
choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file;
encrypting the first key, K_1 , and the unique identifier with a second key, K_2 , to generate a first value;
encrypting the requested file with the first key, K_1 , to generate a second value; and
transferring the first and second values.
2. (ORIGINAL) The method of claim 1, wherein the requested file is an encrypted file.
3. (ORIGINAL) The method of claim 1, further comprising transferring the first key, K_1 , upon a payment being made.
4. (ORIGINAL) The method of claim 3, further comprising decrypting the second value with the first key, K_1 , to generate the requested file.
5. (ORIGINAL) The method of claim 1, further comprising interrupting the transmission of the second value.

6. (ORIGINAL) The method of claim 5, further comprising continuing the transmission of the second value without retransferring the entire second value.

7. (Previously Presented) The method of claim 1, wherein the second key, K_2 is a public key having a corresponding private third key, K_3 .

8. (ORIGINAL) The method of claim 1, wherein the unique identifier is an MD5 checksum of the requested file.

9. (ORIGINAL) The method of claim 1, wherein the unique identifier corresponds to binary information.

10. (ORIGINAL) The method of claim 1, wherein the unique identifier corresponds to ASCII information.

11. (WITHDRAWN) A method for transferring files, comprising:
receiving a request to continue downloading a partially transferred encrypted file;
receiving a first value corresponding to an encrypted quantity wherein the quantity comprises a first key, K_1 , and a first unique identifier corresponding to unencrypted form of the encrypted file;
recovering the first key, K_1 , and the first unique identifier using a second key, K_2 ;

locating an unencrypted form of the encrypted file based on the first unique identifier;

computing a second unique identifier from the unencrypted form of the encrypted file;

confirming that the first and second unique identifiers are equal;

encrypting the unencrypted form of the encrypted file with the first key, K_1 , to generate the requested encrypted file; and

transferring a remaining portion of the partially transferred encrypted file.

12. (WITHDRAWN) The method of claim 11, further comprising appending the transferred remaining portion with the partially transferred file.

13. (WITHDRAWN) The method of claim 12, further comprising transferring the first key, K_1 , upon a payment being made.

14. (WITHDRAWN - Previously Presented) The method of claim 13, further comprising decrypting the appended file with the first key, K_1 .

15. (WITHDRAWN) The method of claim 11, further comprising interrupting the transmission of the remaining portion of the partially transferred encrypted file.

16. (WITHDRAWN) The method of claim 15, further comprising continuing the transmission of the remaining portion of the partially transferred encrypted file.

17. (WITHDRAWN) The method of claim 11, wherein the second key, K_2 , is a public key having a corresponding private third key, K_3 .

18. (WITHDRAWN) The method of claim 11, wherein the first and second unique identifiers are MD5 checksums.

19. (WITHDRAWN) The method of claim 11, wherein the unique identifier corresponds to binary information.

20. (WITHDRAWN) The method of claim 11, wherein the unique identifier corresponds to ASCII information.

21. (WITHDRAWN) A method for verifying downloaded files, comprising;
receiving a first unique identifier corresponding to a downloaded encrypted file, wherein the encrypted file was computed using a first key, K_1 ;
receiving a first encrypted value computed using a second key, K_2 , wherein the encrypted value contains information relating to a second unique identifier and the first key, K_1 ;
extracting the second unique identifier and the first key, K_1 , using a third key, K_3 ;
retrieving a third unique identifier corresponding to a verified file having the second unique identifier;
confirming that the first and third unique identifiers are equal; and
transferring the first key, K_1 .

22. (WITHDRAWN) The method of claim 21, wherein the first, second, and third unique identifiers are MD5 checksums.

23. (WITHDRAWN - Previously Presented) The method of claim 21, wherein the second key, K_2 is a public key and the third key is a private key.

24. (WITHDRAWN) The method of claim 21, wherein the first, second, and third unique identifiers corresponds to binary information.

25. (WITHDRAWN) The method of claim 21, wherein the unique identifier corresponds to ASCII information.

26. (WITHDRAWN) The method of claim 21, further comprising decrypting the downloaded encrypted file using the first key, K_1 .

27. (WITHDRAWN) The method of claim 21, further comprising locating an unencrypted form of the encrypted file based on the second unique identifier, computing an encryption of the located unencrypted form of the encrypted file with the first key, K_1 , and computing the third unique identifier from the computed encryption.

28. (Previously Presented) An apparatus for transferring binary files, comprising:

means for receiving a request to transfer a file;

means for locating the requested file stored in a memory;

means for computing a unique identifier corresponding to the requested file;

means for choosing a first key, K_1 , wherein the first key, K_1 , is unique to the particular transfer of the requested file;

means for encrypting the first key, K_1 , and the unique identifier with a second key, K_2 , to generate a first value;

means for encrypting the requested file with the first key, K_1 , to generate a second value; and

means for transferring the first and second values.

29. (ORIGINAL) The apparatus of claim 28, wherein the requested file is an encrypted file.

30. (ORIGINAL) The apparatus of claim 28, further comprising means for transferring the first key, K_1 , upon a payment being made.

31. (ORIGINAL) The apparatus of claim 30, further means for comprising decrypting the second value with the first key, K_1 , to generate the requested file.

32. (ORIGINAL) The apparatus of claim 28, further comprising means for interrupting the transmission of the second value.

33. (ORIGINAL) The apparatus of claim 32, further comprising means for continuing the transmission of the second value without retransferring the entire second value.

34. (Previously Presented) The apparatus of claim 28, wherein the second key, K_2 , is a public key having a corresponding private third key, ~~K_3~~ K_3 .

35. (ORIGINAL) The apparatus of claim 28, wherein the unique identifier is an MD5 checksum of the requested file.

36. (ORIGINAL) The apparatus of claim 28, wherein the unique identifier corresponds to binary information.

37. (ORIGINAL) The apparatus of claim 28, wherein the unique identifier corresponds to ASCII information.

38. (WITHDRAWN) An apparatus for transferring binary files, comprising;
means for receiving a request to continue downloading a partially transferred encrypted file;

means for receiving a first value corresponding to an encrypted quantity wherein the quantity comprises a first key, K_1 , and a first unique identifier corresponding to unencrypted form of the encrypted file;

means for recovering the first key, K_1 , and the first unique identifier using a second key, K_2 ;

means for locating an unencrypted form of the encrypted file based on the first unique identifier;

means for computing a second unique identifier from the unencrypted form of the encrypted file;

means for confirming that the first and second unique identifiers are equal;

means for encrypting the unencrypted form of the encrypted file with the first key, K_1 , to generate the requested encrypted file; and

means for transferring a remaining portion of the partially transferred encrypted file.

39. (WITHDRAWN) The apparatus of claim 38, further comprising means for appending the transferred remaining portion with the partially transferred file.

40. (WITHDRAWN) The apparatus of claim 39, further comprising means for transferring the first key, K_1 , upon a payment being made.

41. (WITHDRAWN - Previously Presented) The apparatus of claim 40, further comprising means for decrypting the appended file with the first key, K_1 .

42. (WITHDRAWN) The apparatus of claim 38, further comprising means for interrupting the transmission of the remaining portion of the partially transferred encrypted file.

43. (WITHDRAWN) The apparatus of claim 42, further comprising means for continuing the transmission of the remaining portion of the partially transferred encrypted file.

44. (WITHDRAWN) The apparatus of claim 38, wherein the second key, K_2 , is a public key having a corresponding private third key, K_3 .

45. (WITHDRAWN) The apparatus of claim 38, wherein the first and second unique identifiers are MD5 checksums.

46. (WITHDRAWN) The apparatus of claim 38, wherein the unique identifier corresponds to binary information.

47. (WITHDRAWN) The apparatus of claim 38, wherein the unique identifier corresponds to ASCII information.

48. (WITHDRAWN) An apparatus for transferring binary files, comprising;
means for receiving a first unique identifier corresponding to a downloaded encrypted file, wherein the encrypted file was computed using a first key, K_1 ;
means for receiving a first encrypted value computed using a second key, K_2 , wherein the encrypted value contains information relating to a second unique identifier and the first key, K_1 ;
means for extracting the second unique identifier and the first key, K_1 , using a third key, K_3 ;
means for retrieving a third unique identifier corresponding to a verified file having the second unique identifier;
means for confirming that the first and third unique identifiers are equal; and
means for transferring the first key, K_1 .

49. (WITHDRAWN) The apparatus of claim 48, wherein the first, second, and third unique identifiers are MD5 checksums.

50. (WITHDRAWN - Previously Presented) The apparatus of claim 48, wherein the second key, K_2 is a public key and the third key is a private key.

51. (WITHDRAWN) The apparatus of claim 48, wherein the first, second, and third unique identifiers corresponds to binary information.

52. (WITHDRAWN) The apparatus of claim 48, wherein the unique identifier corresponds to ASCII information.

53. (WITHDRAWN) The apparatus of claim 48, further comprising means for decrypting the downloaded encrypted file using the first key, K_1 .

54. (WITHDRAWN) The apparatus of claim 48, further comprising means for locating an unencrypted form of the encrypted file based on the second unique identifier, means for computing an encryption of the located unencrypted form of the encrypted file with the first key, K_1 , and means for computing the third unique identifier from the computed encryption.

55. (Previously Presented) The method of claim 1, wherein the second value includes a plurality of versions of the requested file.

56. (Previously Presented) The method of claim 55, wherein each version of the requested file differs in quality.

57. (Previously Presented) The apparatus of claim 28, wherein the second value includes a plurality of versions of the requested file.

58. (Previously Presented The apparatus of claim 57, wherein each version of the requested file differs in quality.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None